Arresting Wormhole Attack in Ad hoc Network using Cumulative Threshold Transmission Rate

S. Vijayalakshmi
Dept. of MCA
Hindustan University
Chennai, India

P. Annadurai
Dept. of Computer Science
Kanchi Mamunivar Centre for Post
Graduate Studies (Autonomous),
Puducherry, India

ABSTRACT

A mobile ad hoc network is a collection of mobile nodes that are interconnected via a wireless medium forwards packet to other nodes through multi hop mechanism. The genuine intermediaries relay the packets intended for the indirect radio range destination node. The cooperation existing between the intermediate nodes acts as a strong determinant for successful routing in ad hoc network. The association between these nodes can be weakened by the advent of wormhole adversary inside the network. This adversary tries to deteriorate the routing fabric embedded in this network by short circuiting the normal flow of packets through a resource enriched out of band channel exclusively dedicated for this purpose. Two wormhole adversaries collude to achieve this mission and the strong association between them dampens the robust routing protocols designed for effective routing in ad hoc network. The nefarious nexus between the colluders can be amputated by invoking a host of novel remedial measures as proposed in this paper. The comparison between the Cumulative Transmission Rate and Threshold Transmission Rate, mismatch in ROUTE CACHE value, ACKNOLWDGEMENT packet hop count are a few to thwart the occurrence of wormhole attack in ad hoc network. Deploying a suitable agent to monitor and circumvent the spurious activity if exceeding a specific threshold is also enrolled. Suitable graphs have been simulated to endorse the research idea proposed in this paper.

General Terms

Mobile Ad hoc Network, Security, Wormhole Attack, Countermeasure

Keywords

Mobile Ad hoc Network, Wormhole Attack, Agent, Cumulative Transmission Rate, Route Cache Change Rate.

1. INTRODUCTION

In multihop wireless systems, the need for cooperation among nodes to relay each other's packets exposes them to a wide range of security attacks. A particularly devastating attack is the wormhole attack, where a malicious node records control traffic at one location and tunnels it to a colluding node, possibly far away, which replays it locally. This can have an adverse effect on route establishment by preventing nodes from discovering legitimate routes that are more than two hops away. Previous works on tolerating wormhole attacks have focused only on detection and used specialized hardware, such as directional antennas or extremely accurate clocks. There are many unsolved problems in ad hoc networks; security being one of the major concerns. The wormhole attack is among the most threatening and dangerous attacks on these types of network. The dynamic and cooperative nature of ad hoc networks presents substantial challenges in securing and detecting attacks in these networks [1].A Wireless ad-hoc network is a temporary network set up by wireless mobile computers moving arbitrary in the places that have no network infrastructure. Due to security vulnerabilities of the routing protocols, wireless ad-hoc networks are unprotected to attacks of the malicious nodes. The wormhole attack is possible even if the attacker has not compromised any hosts and even if all communication provides authenticity and confidentiality. The wormhole attack can form a serious threat in wireless networks, especially against many ad hoc network routing protocols and location-based wireless security systems. For example, most existing ad hoc network routing protocols, without some mechanism to defend against the wormhole attack, would be unable to send routes longer than one or two hops, severely disrupting communication[2].

Among all the research issues, security is an essential requirement in ad hoc networks. Compared to wired networks, MANETS are more vulnerable to security attacks due to the lack of a trusted centralized authority, easy eaves dropping because of shared wireless medium, dynamic network topology, low bandwidth, battery power and memory constraints of the mobile devices [3].

The rest of the paper is organized as follows. Section 2 discusses the wormhole attack in detail and the wormhole attack model. Section 3 proposes appropriate countermeasure for ad hoc network. Section 4 presents empirical results and discussions. Finally, we make some conclusions and future direction in Section 5.

2. WORMHOLE ATTACK – SUBTLE INTRODUCTION

A mobile ad hoc network with its unique characteristics is plagued by a host of security threats from within and outside the network. Despite providing defense in depth security cover/architecture for the network, it is open to a slew of security incidents from the intruders who consciously manipulate the routing process associated with this network. One such prominent attack is wormhole attack which is exploiting the network to act against itself. This can be perpetuated in two modes viz. encapsulated and out of band channel [4][5]. The real intent of the attacker is not in information tampering but in mass divulgence of the data to the unauthorized network members.

During the attack, a malicious node captures packets from one location in the network, and ‘‘tunnels’’ them to another malicious node at a distant point, which replays them locally. The tunnel can be established in many different ways, such as through an out-of-band hidden channel (e.g., a wired link), packet encapsulation, or high powered transmission. This tunnel makes the tunneled packet arrive either sooner or with lesser number of hops compared to the packets transmitted over normal multihop routes. This creates the illusion that the two end points of the tunnel are very close to each other. A wormhole tunnel can actually be useful if used for forwarding all the packets [6] [7]. However, in its malicious incarnation, it can be used by the two malicious end points of the tunnel to pass routing traffic to attract routes through them. The malicious end points can then launch a variety of attacks against the data traffic flowing on the wormhole, such as the grayhole attack or statistical flow analysis of the traffic. Also the wormhole attack can affect route establishment by preventing any two nodes in the network that are greater than two hops away from discovering routes to each other. The wormhole attack affects many applications and utilities in ad hoc networks such as, network routing, data aggregation and clustering protocols, and location based wireless security systems. Finally, the wormhole attack is considered particularly insidious since it can be launched without having access to any cryptographic keys or compromising any legitimate node in the network [8] [9].

2.1 Types of Wormhole Attack

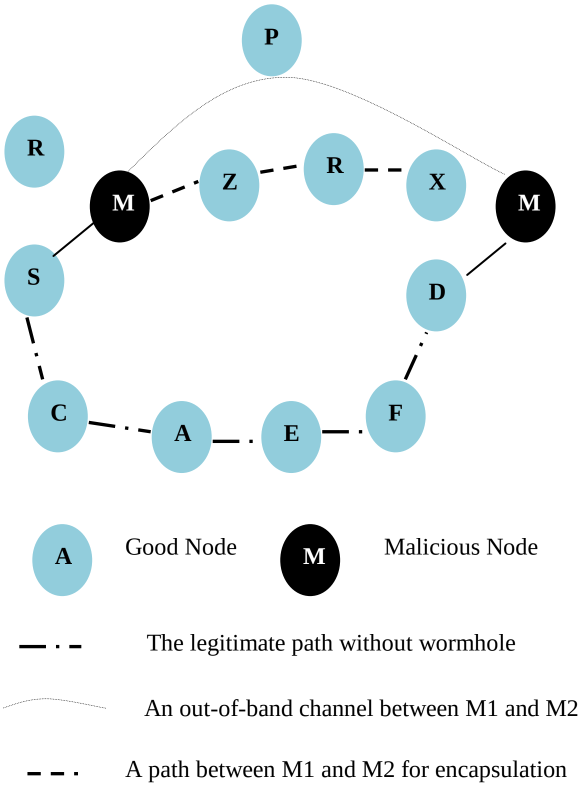

P
R
M
Z
R
X
M
S
D
C
A
E
F
A
Good Node
M
Malicious Node
The legitimate path without wormhole
An out-of-band channel between M1 and M2
A path between M1 and M2 for encapsulation

Fig 1: Wormhole Attack Formation

In the first method for establishing the tunnel shown in Figure 1, a malicious node denoted M in the figure, encapsulates a packet received from its neighboring node S. Node M then sends the encapsulated packet to the colluding malicious node N. Node N then replays the packet in its neighborhood after decapsulating the packet. Thus, the original packet transmitted by node S in its neighborhood is replayed by node N in its neighborhood, which includes node D. For example, if the original packet transmitted by node S (and tunneled by node M) was a hello packet, then node N on receiving this packet would assume that node M is its neighbor, which is not true. As another example, if node S transmits a route request packet for node D, then node M can “tunnel” such a packet to node N by encapsulating the packet [10]. As a result, this route request packet will arrive at the destination node D with a lower hop count than the other Route Request packet going through the other route. This happens in spite of using any secure routing protocol such as the one given earlier. Note that nodes between M and N that relay the packet cannot interpret the packet as it is encapsulated. Therefore, they cannot increment the hop count [11].

In the second method for establishing the tunnel shown in Figure 1, the two malicious nodes M and N are assumed to have access to an out-of-band high bandwidth channel. This could be achieved for example by having a wired link between the two nodes or by having a long range high bandwidth wireless link operating at a different frequency. Thus, this method requires specialized hardware capability and hence is more difficult than the previous method. In this case also, a hello packet transmitted by node S can be retransmitted in the vicinity of node D. As a result node D infers that node S is its neighbor. Similarly, a route request packet, from node S for node D, can also reach node D (which is the destination for the route request packets) faster and possibly with fewer hops, since a high-bandwidth direct link is being used between the two malicious nodes [12][13]. As a result, the two endpoints of the tunnel can appear to be very close to each other. To see this, consider Figure 1. Here node D receives three route requests. It is clear that the route request received through the wormhole will have the least hops.

It seems as if the malicious nodes are performing a useful service by tunneling the packets. This would be so if the nodes were performing this service without any malicious intent, but malicious nodes could use this attack to undermine the correct operation of various protocols in ad hoc networks. The most important protocol that is impacted is the routing protocol, as we can see from the examples given earlier. Data aggregations, protocols that depend on location information, data delivery, and so on, are some other examples of services that can be impacted. Note that the wormhole attack can be successful even without access to any cryptographic material on the nodes [14] [15].

2.2 Wormhole Attack Model

Figure 2 conceptualizes the wormhole attack model where the wormhole adversaries in the mobile ad hoc network conspiring to bypass the normal flow of data packets to a foreign network populated by a group of unauthorized members wishing to avail the network services through illegitimate way.

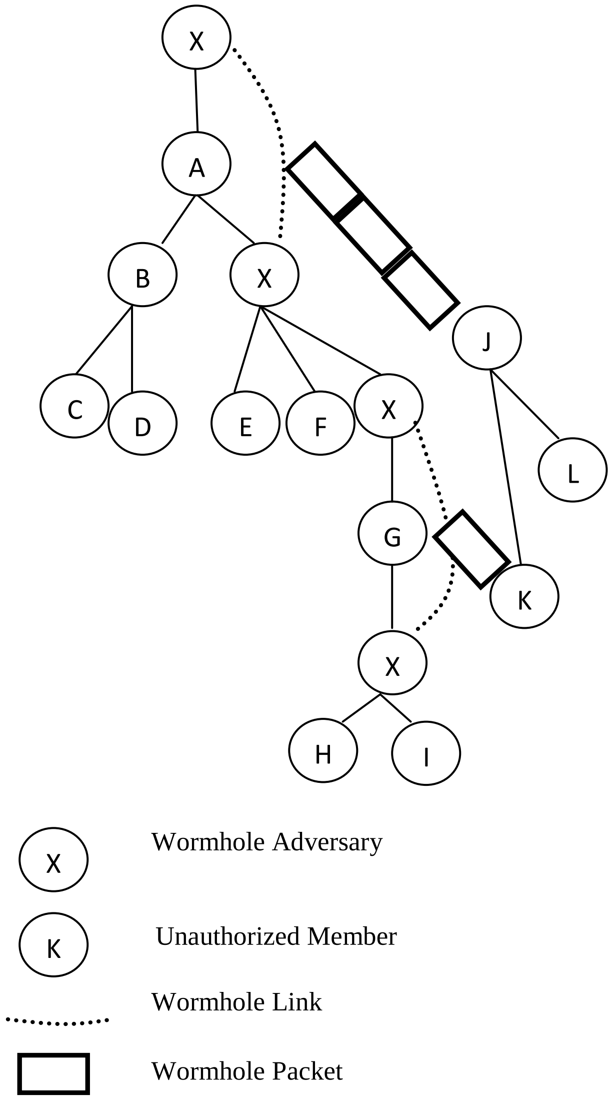


Fig 2: Wormhole Attack Model

3. ARRESTING WORMHOLE ATTACK IN ADHOC NETWORK USING CUMULATIVE THRESHOLD TRANSMISSION RATE

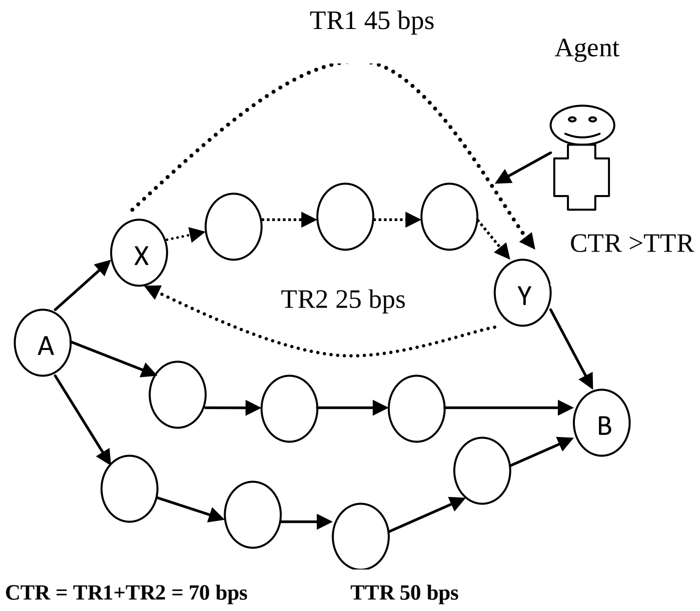
Wormhole attack in ad hoc network can be instantiated in two modes viz one in-band wormhole link where the packet encapsulation technique comes to the fore, the other is out of band tunnel where the attackers engage in active packet exchange through an resource enriched sophisticated channel equipped with special hardware capability. The transmission rate (TR) is defined as the number of packets of data sent/processed per unit block of time. TR is defined as the speed at which a network device communicates within the network.

Effective transmission rate associated with the wormhole adversaries tends to surge in anticipation of the packets exchange spree through the tunnel. The resource enriched tunnel draws the attention of the monitoring agent that intermittently checks and calculates the network centric features like TR, bandwidth, delay, hop count etc. The data processing speeds of the participating culprit nodes in the tunnel ie Cumulative Transmission Rate (CTR) of the forward and backward link is calculated and is compared against the Threshold Transmission Rate (TTR) set during the initiation/TCP handshaking phase. The CTR is surely expected to go beyond the agreed rate/level to influence the data traffic through the tunnel/encapsulated path and to speedily transmit the data frames to the destination or the other colluder with minimal chance of being booked by the other genuine nodes prevailing in the network.

The criminal conspiracy between the two associated wormhole colluders can be brought to light by either the genuine neighbor set/group or the agent continuously monitoring the network for sporadic occurrence of network misbehavior/crime. The key Master agent captures and records the suspicious activities happening within its vicinity which may not be the case always. The deployed/polled slave agent monitors closely the network misbehavior occurring within its range and raises a signal to other trustable nodes that surrounds it and to the master agent. The existence of end to end encapsulation does not repel any intruder from cracking the route encryption that amounts to packets taking an excessive journey through an out of band channel. The timely arrival of acknowledgement packets from the destination node ensures the safe transit of packet through the established and approved/recommended path (ERP).

The marginal decrease in the network performance metric like end to end delay, Acknowledgement Packet hop count from the destination node (RREP) routed through the wormhole guarantees the presence of colluding adversaries resulting in excessive passage of the packet through a resource enriched out of band channel. The prevalence of abnormal network metrics guarantees the presence of intruders, who consistently and constantly flout the network rules, protocols and architecture etc. The trustable node set (TNS) surrounding the affected/wormhole infected region maps the region as wormhole jammed zone and tries to freeze it where no productive activities is in place. The intermediate node tries to justify the credibility of the established route by comparing the ROUTE CACHE of the initial Route Request (RREQ), Route Response (RREP) packets and the Route transit packets. The surrounding TNS nodes on sensing a deviation in the ROUTECACHE of the tunneled packets alerts the neighbors about the presence of wormhole attack in its vicinity.

The visualization of the remedial countermeasures for resolving wormhole attack in ad hoc network is illustrated through a series of figure from Figure 3 to 7. Figure 3 picturizes the agent sensing a discrepancy in CTR and TTR and eventually blacklisting nodes X and Y. Figure 4 and 5 portrays a ROUTECACHE mismatch during initial RREQ and RREP phases in the presence of wormhole attack in ad hoc network. Figure 6 and 7 depicts the discrepancy in Acknowledgement packet hop count during RREP phase in the presence and absence of wormhole attack.



If CTR>TTR Agent Prosecutes the link

CTR - Cumulative Transmission Rate

TTR - Threshold Transmission Rate Set during Handshaking phase

TR1 - Transmission Rate of the forward link

TR2 - Transmission Rate of the backward link

Fig 3: Agent sensing a discrepancy in CTR and TTR and tries to blacklist nodes X and Y

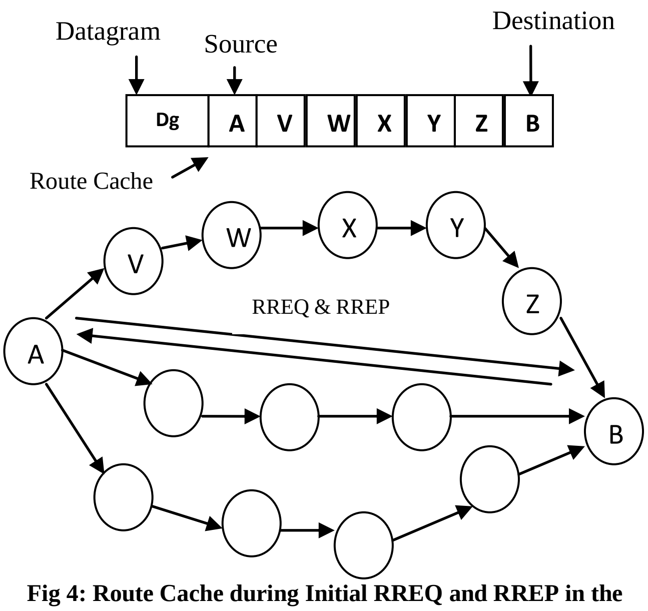


Fig 4: Route Cache during Initial RREQ and RREP in the absence of wormhole attack

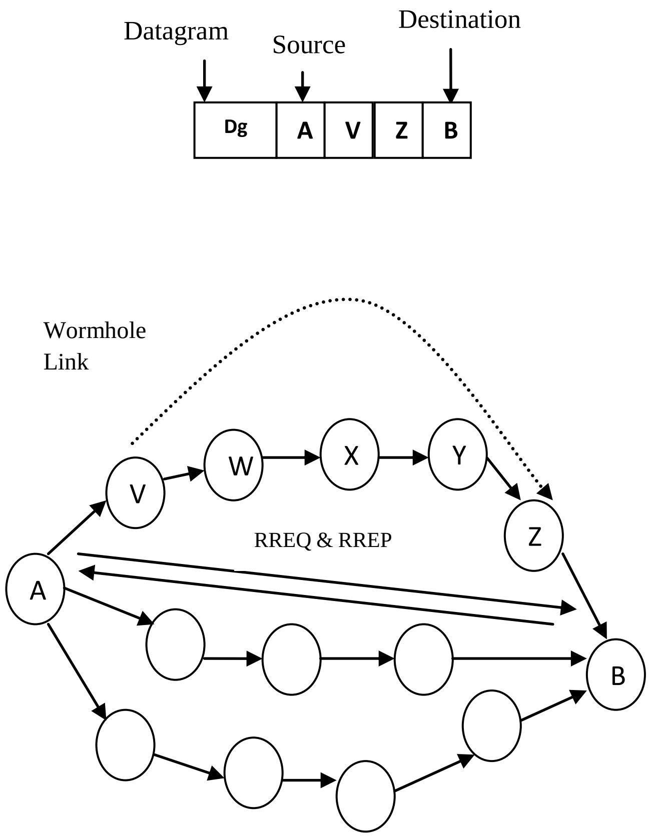


Fig 5: Route Cache Mismatch in presence of wormhole attack

4. EMPIRICAL RESULTS AND DISCUSSIONS

The impact on RC^{2}R is so huge that the wormhole attacker influences/coerces the already destined packets to follow an alternate resource rich (sophisticated) route thereby incurring a Route Cache change (RCC). The route reconfiguration and reconstruction cost due to RCC is so devastating that if left unnoticed leads to excessive wastage of network resources. The adoption of the proposed technique paves way for route rehabilitation at an early phase and thwarts the occurrence of the wormhole attack at any cost. The increase in RC^{2}R value is attributed to the absence of the proposed solution in the wormhole infected zone. Deployment of the proposed countermeasure in the afflicted zone encourages the plummeting nature of RC^{2}R values. Suitable graphs have been simulated using Network Simulator tool under various network conditions and the research findings are evaluated using the proposed countermeasure. Figure 8 and 9 portrays the trend in RC^{2}R values in the absence and presence of proposed solutions.

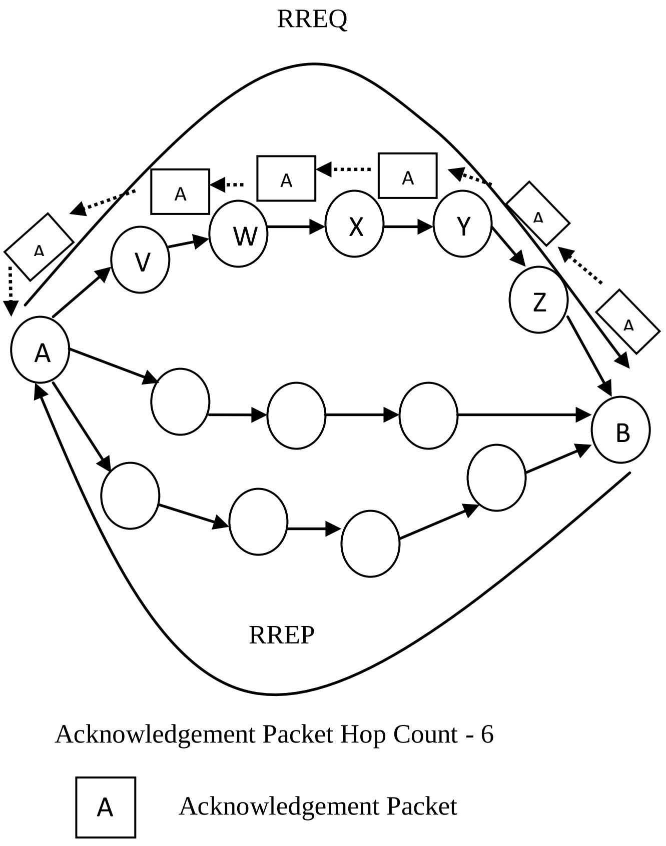


Fig 6: Acknowledgement Packet Hop Count during RREP in absence of wormhole attack

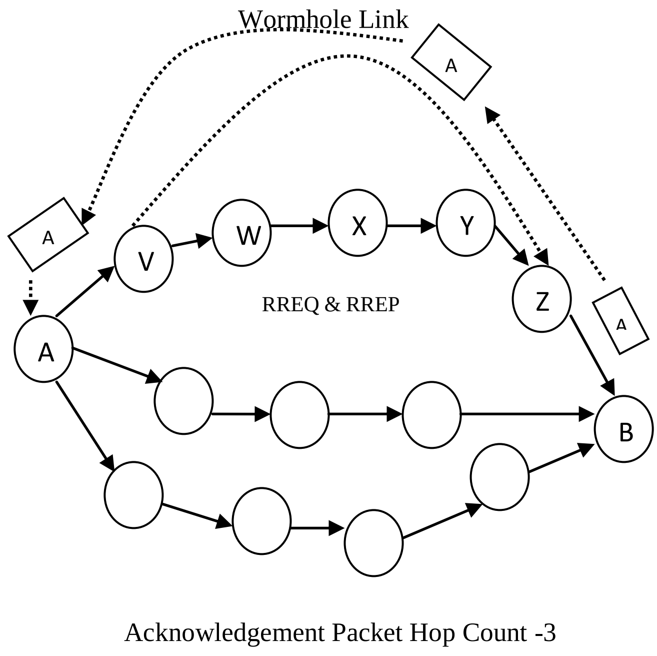


Fig 7: Acknowledgement Packet Hop Count Mismatch during RREP in presence of wormhole attack

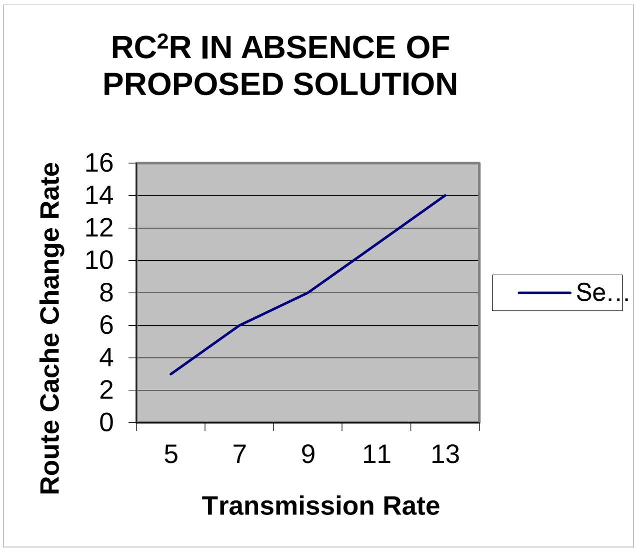


Fig 8: RC^{2}R in absence of proposed solution

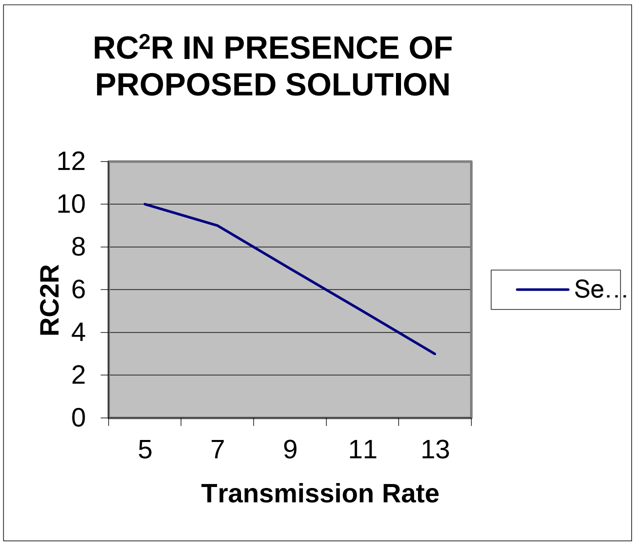


Fig 9: RC^{2}R in presence of proposed solution

5. CONCLUSION AND FORESEEABLE ENHANCEMENT

Appropriate countermeasures/security antidote has been suggested to nail the occurrence of the wormhole attack in ad hoc network by the deployment of agent. The surge in transmission rate of the associated wormhole attackers is attributed to its avariciousness to scan the tunneled data packets and replaying it locally. Suitable graphs have been simulated to evaluate the research deliverables of this work. The performance penalty inflicted on the ad hoc network due to agent's communication, storage and computation complexity has to be taken into consideration. The tradeoff analysis has to be conducted between the complexities associated with the agent and the quantum of performance improvement by the adoption of it. The agent assistance to wormhole infected route rehabilitation; reconfiguration and reconstruction would be the foreseeable enhancement. A proper division of labor mechanism should be in place to distribute evenly the activities of the agent that are near to the wormhole infected zone and the rest.

6. REFERENCES

[1] M.Jain, H.Kandwal, "A Survey on Complex Wormhole Attack in Wireless Ad Hoc Networks", in the Proceedings of the International Conference on Advances in Computing, Control, & Telecommunication Technologies, 2009. ACT '09. December 2009,pp.555-558

[2] Jamil Ibriq, Imad Mahgoub and Mohammad Ilyas, "Secure Routing in Wireless Sensor Networks", 2010, Handbook of Information and Communication Security, Part E, Pages 553-578

[3] Saurabh Upadhyay and Brijesh Kumar Chaurasia, "Detecting and Avoiding Wormhole Attack in MANET Using Statistical Analysis Approach", Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, 1, Volume 84, Advances in Computer Science and Information Technology. Networks and Communications, Part 2, Pages 402-408.

[4] Tassos Dimitriou and Athanassios Giannetsos, "Wormholes No More? Localized Wormhole Detection and Prevention in Wireless Networks", Lecture Notes in Computer Science, 2010, Volume 6131, Distributed Computing in Sensor Systems, Pages 334-347

[5] Manoj V., Raghavendiran N., Aaqib M. and Vijayan R., "Trust Based Certificate Authority for Detection of Malicious Nodes in MANET", Communications in Computer and Information Science, 1, Volume 269, Global Trends in Computing and Communication Systems, Pages 392-401

[6] Marianne A.Azer, Sherif M. El-Kassas, Magdy S. El-Soudani, "A Full Image of the Wormhole Attacks Towards Introducing Complex Wormhole Attacks in Wireless Ad Hoc Networks", in International Journal of Computer Science and Information Security, Special Issue, May 2009**.**

[7] Azer, M.A. El-Kassas, S.M, El-Soudani, M.S., "Immuning Routing Protocols from the Wormhole Attack in Wireless Ad Hoc Networks", Fourth International conference on Systems and Networks Communications, 2009. ICSNC '09, 20-25 Sept. 2009

[8] S.Vijayalakshmi, S.Albert Rabara, "Weeding Wormhole Attack in MANET Multicast Routing Using Two Novel Techniques – LP3 and NAWA2", International Journal of Computer Applications, (0975 - 8887) Volume 16□ No.7, February 2011

[9] S.Xu, and V.B.Bopanna, "On Mitigating In-band wormhole Attack s in Mobile Adhoc Networks", ICC, IEEE Communications Society 2007.

[10] J.D.Parmar., A.D.Patel., R.H.Jhaveri and B.I.Shah., "MANET Routing Protocols and Wormhole Attack against AODV", International Journal of Computer Science and Network Security, Vol.10, No. 4, April 2010.

[11] N.Shanti., L.Ganesan., and K.Ramar., "Study of Different Attacks on Multicast MANET," Journal of Theoretical and Applied Information Technology, 2005-09.

[12] Roy S., Addada V.G., Setia S. and Jajodia S.,"Securing MAODV: Attacks and Countermeasures", Centre for Secure Information Systems, George Mason University, Fairfax, VA 22030.

[13] Yang, H., Luo, H., Ye, F., Lu, S., and Zhang, L.,Security in Mobile Ad hoc Networks: Challenges and Solutions", UCLA Computer Science Department.

[14] Marti, S., Giuli, T.J., Lai, K., and Baker, M.,"Mitigating Routing Misbehavior in Mobile Ad hoc Networks", Department of Computer Science, Stanford University.

[15] Nguyen, H.L. and Nguyen, U.T., "Different Types of Attacks on Multicast in Mobile Ad hoc Network", Ad hoc Networks 6(2008) pages 32-46.